



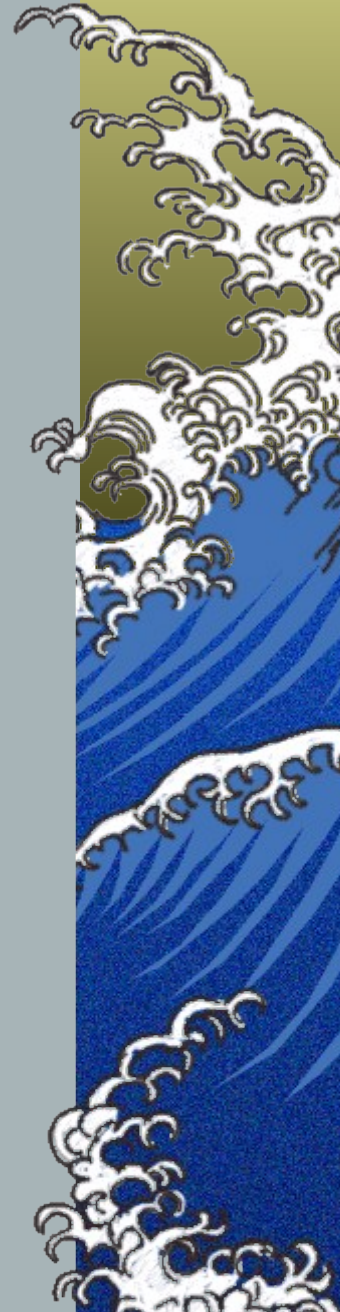
NPMOC Yokosuka

Annual Security Refresher Training

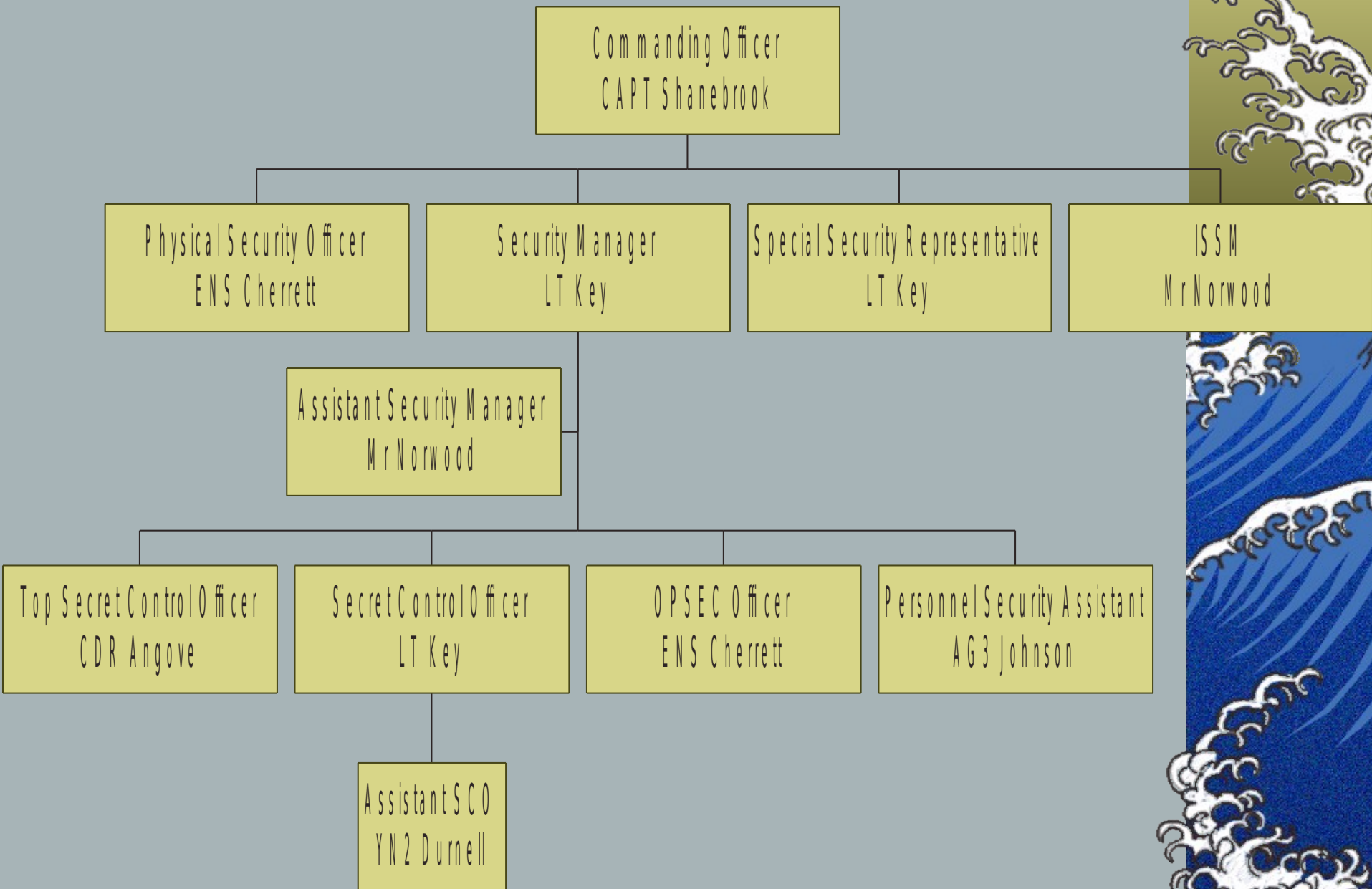


Overview

- *Organization*
- *References*
- *Threats*
- *Responsibility*
- *Clearance vs Access*
- *Visitor Policy*
- *Custody*
- *Storage*
- *Destruction*
- *Incidents*



NPMOC Yokosuka Security Organization



References

- ▶ *SECNAVINST 5510.30A*
(Personnel Security Program)
- ▶ *SECNAVINST 5510.36*
(Information Security Program)

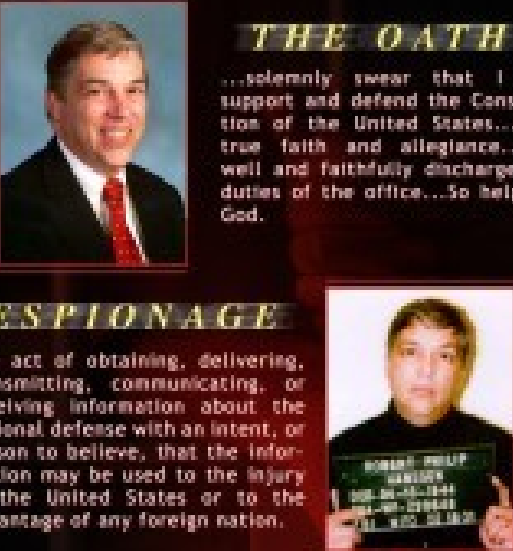


The Threats



Espionage

✦ *In the last 20 years, 80% of all espionage cases have been insiders!*



THE OATH

...solemnly swear that I will support and defend the Constitution of the United States...bear true faith and allegiance...will well and faithfully discharge the duties of the office...So help me God.

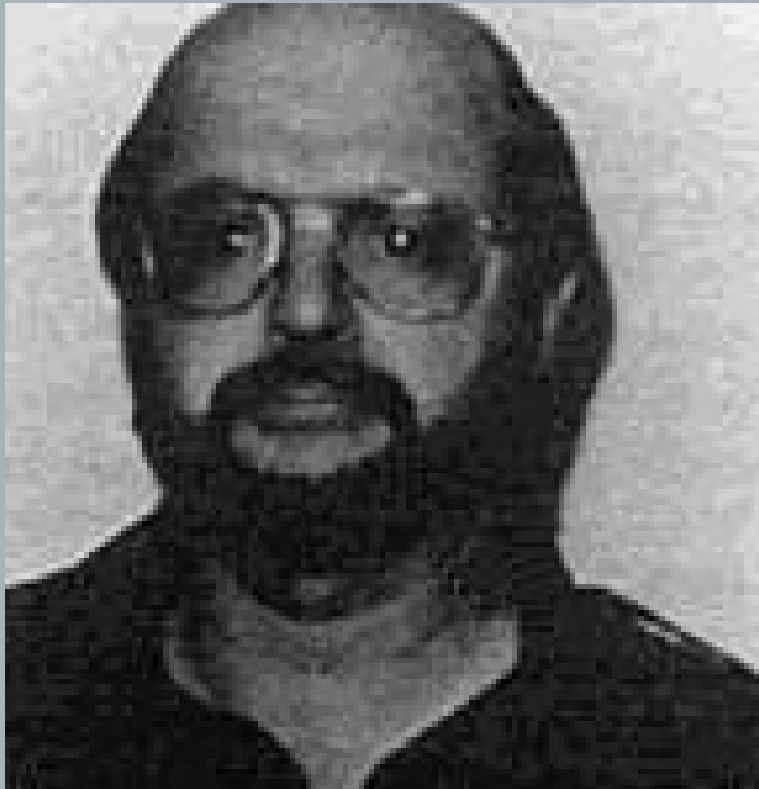
ESPIONAGE

The act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent, or reason to believe, that the information may be used to the injury of the United States or to the advantage of any foreign nation.

Robert P. Hanssen
Spy • Traitor • Deceiver

Office of the National Counterintelligence Executive

Espionage

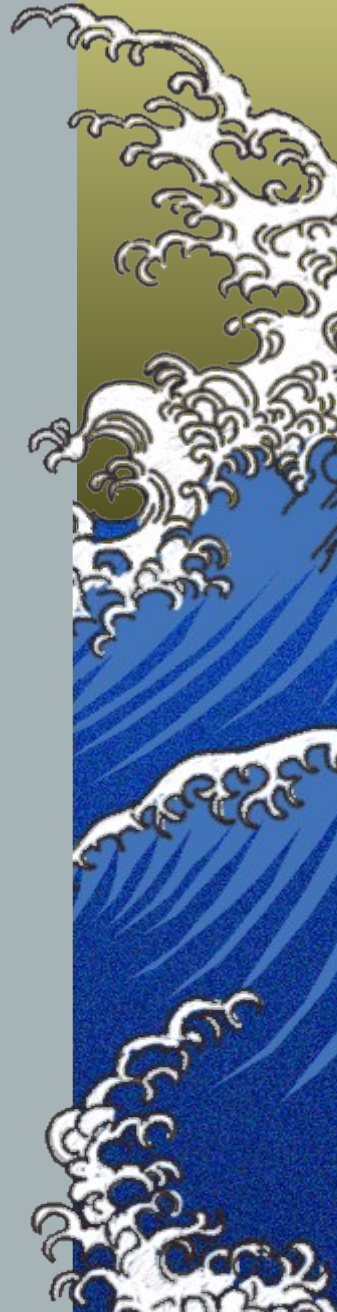


✦ *Espionage can have a devastating effect on our Nation's security.*



Terrorism

✦ *There are people out there that want nothing more than to kill you.*



Carelessness

✦ *Just as
devastating as
deliberate
compromise!*



Responsibility



Protection

- ✦ *All military personnel, regardless of access level, are required to protect and safeguard all classified material.*
- ✦ *If you find improperly secured classified material, you should immediately notify the Security Manager via your Chain of Command.*



Protection

- ★ *Classified material, in any form, is the property of the U.S. Government and is NOT personal property!*

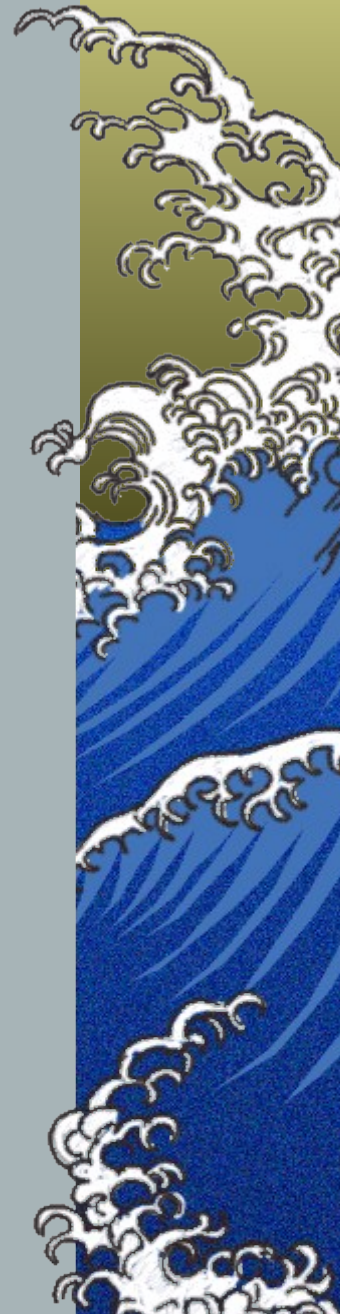


Clearance vs Access



Clearance

- ✦ *A Security Clearance is a formal determination that a person meets the personnel security standards and is eligible for access to classified information other than that in a special access program*
- ✦ *DONCAF is the only Department of the Navy authority that may grant a Clearance*



Access

- ▶ *Access is the ability and opportunity to obtain knowledge of classified information.*
- ▶ *Granted by individual commands*
- ▶ *Need-to-know principle must be followed at all times, regardless of a persons clearance...*



Document

- ▶ *You are responsible for keeping your Security Clearance updated.*
- ▶ *Expeditious and thorough completion of security forms will reduce the process delay for receipt of your clearance.*



Command Visitors

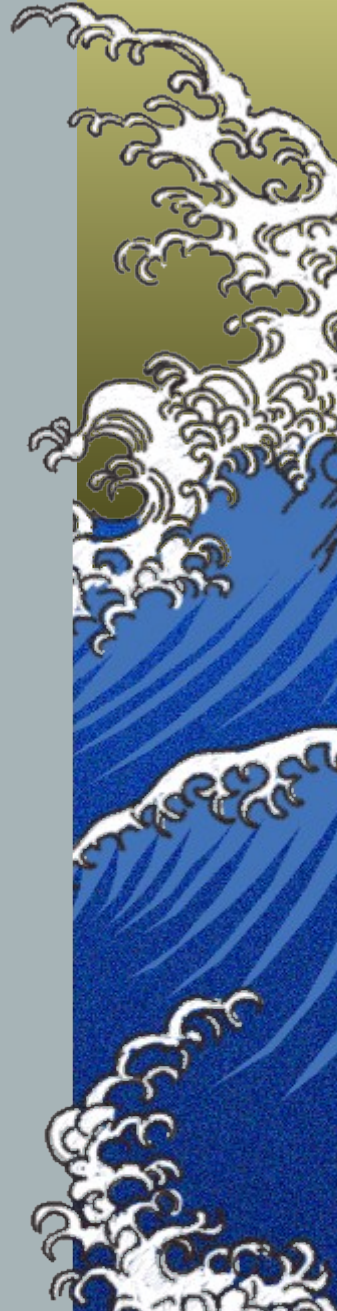


Visitors

- ▶ *All visitors must be admitted by “competent” command authority.*
- ▶ *Uncleared visitors to 2nd deck must be cleared with CDO prior to admittance.*
- ▶ *Challenge any person that you do not know...*
- ▶ *NCIS – authorized up to TS with “Special Agent” badge.*



Material Custody



Custody

- ▶ *Custodians must ensure proper procedures are in place to adequately protect classified material under their control.*
 - ▶ *Procedures must be written*
 - ▶ *Procedures must address*
 - ▶ *Physical Security*
 - ▶ *Check-in/out process*



Custody

- ★ *Custodians will maintain an unbroken chain of custody for all material SECRET and above.*



Storage



Storage

- ★ *TOP SECRET*

- ★ *Closed – SCIF / 2nd Deck*

- ★ *SECRET and below*

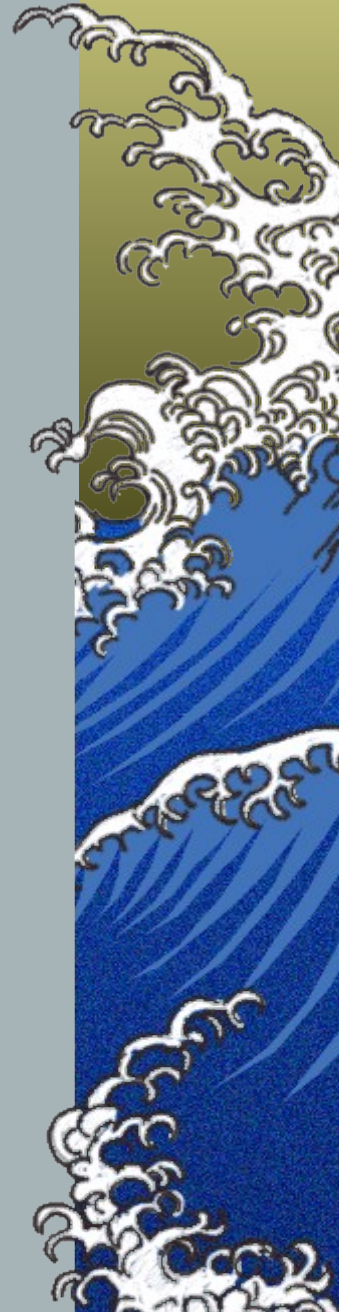
- ★ *Open – 2nd Deck*

- ★ *Closed – 1st / 3rd Deck*



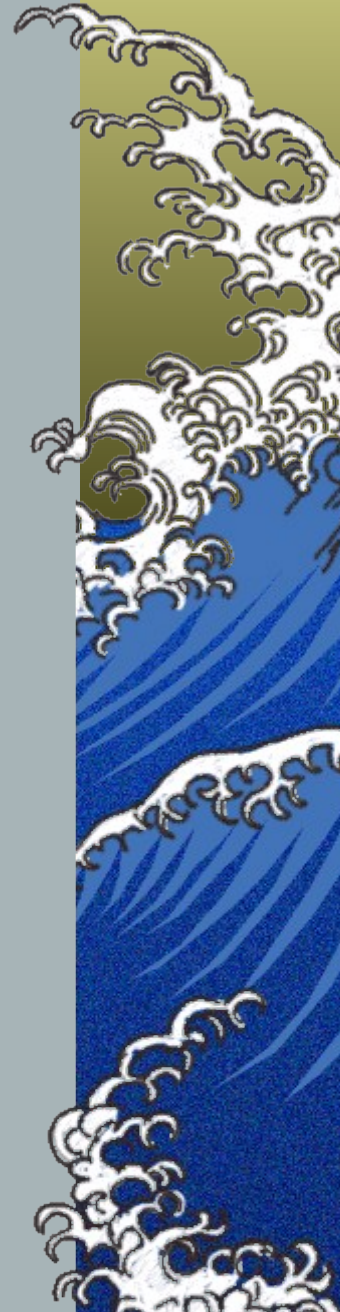
Storage

- ✦ *All safes that contain classified material must have a properly filled out SF 700 (Security Container Information Form).*
 - ✦ *The SF 700 must be kept updated.*
 - ✦ *New combinations are not necessarily required if personnel with access transfer – see the Security Manager if you have questions.*



Storage

- ▶ *All safes that contain classified material must have a properly filled out SF 702 (Security Container Check Sheet).*
 - ▶ *Must be filled in every time a safe is open or closed.*
 - ▶ *Are required to be kept for 30 days.
(Turn in to Security Manager when full)*
 - ▶ *Are required for each COMBINATION, regardless of number of locks.*



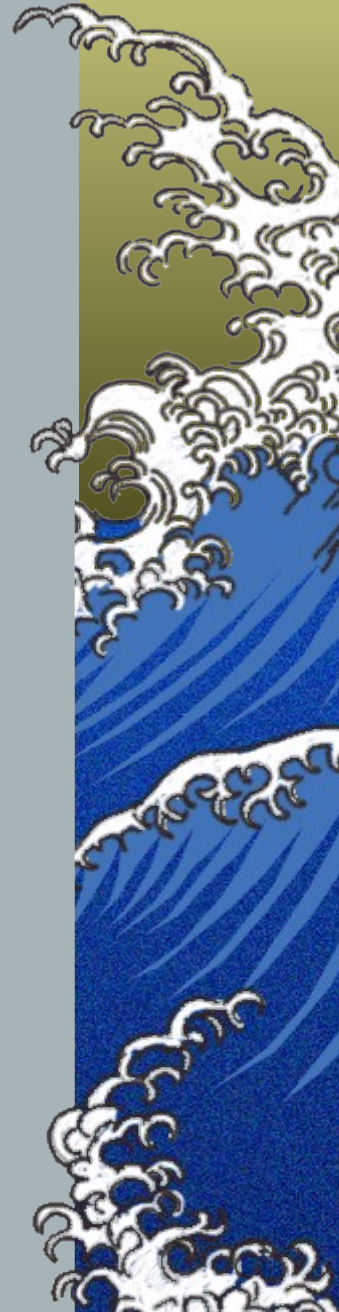
Storage

- ▶ *All spaces that contain classified material must have a SF 701 (Activity Security Check Sheet) attached to the inside of the main access to the space.*
 - ▶ *Defines checkpoints for space shut down.*
 - ▶ *Required to be kept for 30 days. (Turn in to Security Manager when full)*



Storage

- ▶ *All safes that contain classified material must have an inventory of the contents on file (can be located inside safe).*
 - ▶ *KEEP UPDATED.*
 - ▶ *Allows for rapid loss/comprise assessments if safe is found open.*



Destruction



Destruction

- ▶ *Paper / Floppy Disks*
 - ▶ *Shredding*
 - ▶ *Burning*
- ▶ *Hard drives / CD's*
 - ▶ *Draft complete inventory memo and turn over to Security Manager for destruction.*
 - ▶ *CD's may be burned only in emergencies*



Incidents



Reporting

- ✦ *Any individual that becomes aware of a possible loss or compromise of classified material is required to report the situation to the Security Manager or Commanding Officer if the Security Manager is not immediately available.*



Reporting

- ✦ *Any individual with access to classified material must notify their chain of command if approached by foreign nationals seeking information.*

